BOOK CHAPTER | *"Money Matters"*

Bitcoins Usage By Cybercriminals – Evolution And Current Mitigating Approaches

Daniel Tibina Apuri
Digital Forensics & Cyber Security Graduate Programme
Department Of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: dapuri@gimpa.edu.gh
Phone: +233205967243

ABSTRACT

The issue of security is one of the most pressing concerns about the emergence and adoption of cryptocurrencies. There is currently a serious concern regarding the security of blockchain technology. Although cryptocurrencies offer a high level of network security by keeping transactions anonymous, it also raises the possibility of bitcoin being used for illegal reasons. Furthermore, the technology that underpins the operation of a cryptocurrency, like any other information system, is vulnerable to many forms of attacks. A connection where bitcoin is traded for traditional money is a weak spot in the cryptocurrency circulation chain. Because this occurs on newly unregulated exchanges, they are frequently targeted by hackers. Other dangers exist in the bitcoin industry. For example, with the fast appearance of new cryptocurrency exchanges, determining their previous performance and just hoping for their dependability becomes challenging. There are "grey" stock exchanges, which can halt operations at any time after withdrawing assets. The potential of a cryptocurrency to launder money or support terrorists is the most serious security concern for many nations. To combat money laundering, the Japanese government, finance ministers, and chiefs of central banks in France and Germany have proposed making cryptocurrency regulation international. The IMF also believes that worldwide regulatory oversight of the digital currency sector is required.

Keywords: Cryptocurrencies, Blockchain, Security, Transaction, Distributed, Network, Encryption, Privacy, Regulations, Decentralised, Dark Web

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free

Citation: Daniel Tibina Apuri (2022): Bitcoins Usage By Cybercriminals – Evolution And Current Mitigating Approaches Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 251-258
www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P40

1. INTRODUCTION

Cryptocurrencies, (shortened as crypto) are digital resources intended to operate as a means of exchange in comparison to conventional money (currency). They use powerful encryption technologies to secure exchanges, as the name implies. They, like most traditional currencies, have no objective worth; but are rather determined by transactions they are used for.

As a result, cryptocurrencies are notoriously unpredictable. While cryptocurrencies are similar to traditional currencies in certain aspects, they differ in some significant ways. No central authority, such as a national or multinational central bank, has jurisdiction over them. No institution or agency guarantees the currency's value or adds to the system's money supply. The mathematics that is used to validate transactions keeps scarcity alive. Cryptocurrencies are for their very design decentralized, and as a result, they provide a means of exchange that is free of government control. These elements characterize liberal cyber-culture.

A pseudonym, “Satoshi Nakamoto” was the first to propose the notion of cryptocurrency in an academic paper published in 2008 (Nakamoto, 2008; Schatt, 2014). Satoshi Nakamoto's identity, whether being an individual or a community has remained a secret to this day. This made Bitcoin the first and most well-known cryptocurrency in general use. In 2009, the open-source bitcoin program and blockchain network were launched, when the founding block of the bitcoin protocol was generated. Bitcoin has thrived since its conception, with dark websites such as Silk Road, fuelling its early growth. A variety of cryptocurrencies have developed since the birth of Bitcoin. Popular among them after Bitcoin are Ethereum, Litecoin, Ripple, Dogecoin, Binance Coin and Bitcoin Cash. According to coinmarketcap, there are currently about 1,400 different types of cryptocurrencies in use.

The fundamentally untraceable nature of exchanges, as well as the lack of a centralized authority, made it ideal for illicit trading and criminal business. The main goal was to build a distribution mechanism free of governmental or banking authority oversight, based on a mathematical formula rather than "third-party authenticity," where payments may be made virtually in a secure, transparent, and indisputable manner. The implementation of this concept entails a payment system in which all transactions take place explicitly between the sender and receiver and are distributed through a peer-to-peer network. Although the records are public, the user's profile remains a mystery. Each block includes data on the current transaction and the preceding block, and the coin is mined to retrieve data in the form of "blocks." This connects all subsequent blocks to the first.

1.1 Background To The Study

According to Cambridge University academics, there are over three million distinct individuals that use cryptocurrencies on a global scale. Cryptocurrencies are generated on the Internet (which in itself is autonomous and deregulated), distributed in a peer-to-peer (literally from one individual to the other) manner, and protected by encryption. Financial institutions and regulators are no longer required as facilitators. Cryptocurrencies are thereby not tied to any given entity, but instead a 'universal electronic economy,' obviating the possibility of administrative control by design. The creative, unregulated character of cryptocurrencies, as well as the level of anonymity they provide, are all major drivers of rising criminal activity related to them (Bray, 2016).

While the advantages of bitcoins and all other cryptocurrencies have been enormous benefits to their users, the drawbacks cannot be understated. These drawbacks mostly through criminal cyber activities have a huge impact on the global economy and as such respective measures and approaches must be put in place to curb these instances. Much is not known about the mitigating efforts largely because bitcoins and cryptocurrencies are unregulated and untamed.

However, this study seeks to analyse the numerous cybercrimes propelled by bitcoins and cryptocurrencies, what efforts have been put in place to address the same and make recommendations for policy and future research.

2. RELATED LITERATURE

Cryptocurrencies are both targets of cybercrime and a source of payment in criminal operations where the victim must pay, such as extortion, Ponzi schemes, and other investment frauds (Reddy & Minnaar, 2018). Furthermore, cryptocurrencies are used to make payments on the dark web, where tools, data, and services used in cybercrime are traded. Crime-as-a-service is a type of cloud computing used by the criminal underworld. Year after year, cybercrime has increased. Money is the primary motivation. According to Verizon, one of the world's top suppliers of communications and information services, as many as 86 per cent of all successful cyberattacks on their clients in 2020 were aimed at financial gain.

Fig 1: Popular Cryptocurrencies
Source*: https://economictimes.indiatimes.com)*

Bitcoin as a facilitator of cybercrime

Illegal cyber-commerce

The Dark Web and cryptocurrency are the ideal combination for laundering revenues from unlawful services and sales in a rapid, anonymous, and very simple manner (Van Mieghem & Pouwelse, 2015). As a result, it's no surprise that cryptocurrencies have become the preferred method of payment for electronic transactions on the Dark Web (Naik & Serumula, 2015). In 2018, the Canadian Centre for Sanctions and Illicit Finance and cybercrime investigative firm Elliptic collaborated on a study to identify cryptocurrency-related money-laundering typologies. "Darknet markets are a crucial source of illicit funds," according to the study (Fanusie & Robinson, 2018).

Cyber-money laundering

The Financial Crimes Enforcement Network (FinCen) defines money laundering as "making illegally obtained revenues ('dirty money') appear legal ('clean money') by layering or consolidating it with multiple transactions to obscure its true origins. Cryptocurrencies' design and technical foundations do not necessitate all of the above procedures connected with money laundering because they are unregulated and untraceable by nature. However, Fanusie & Robinson (2018) outlined certain conversion facilities that can be used to launder cryptocurrencies.

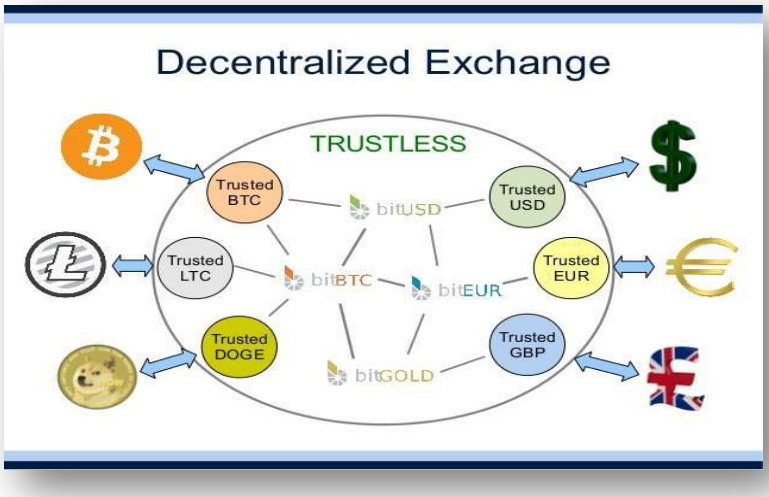

Fig 2: Decentralised Cryptocurrency Exchanges
Source: https://en.bitcoinwiki.org/wiki/DEXes)

The figure above is a depiction of cybercurrencies being exchanged for traditional currencies within no legal framework. Platforms such as Bitshares, Waves, 0x Protocol, EtherDelta, Crypto-exchange, Bitcoin ATM operators, Gambling services, Mixers, and Bitcoin-exchange facilitate these cyber transactions. Tumblers and mixers are the most well-known bitcoin laundering services. Users can deposit their coins into a pool of other cryptocurrencies using these services (Reddy & Minnaar, 2018). In effect, the transfer 'mixes' or 'tumbles' the currency while also rearranging the sender and receiver account identifiers. As a consequence, consumers received newly minted bitcoin addresses, obscuring the money trail much further. This facilitates money movement throughout the Bitcoin system's procedures. However, those who intend to finally trade their bitcoins for cash might make use of further money laundering services. These incognito services enable users to trade bitcoins for conventional currencies through Paypal and Western Union (Ciancaglini et al, 2015).

Bitcoin as a target for cybercriminals

Traditional cybercrime threatens cryptocurrency exchanges, wallet providers, and payment processors. Several cryptocurrency exchanges and payment processors have suffered hacking and phishing assaults, resulting in a loss of Bitcoin and, in some cases, bankruptcy and the closure of the attacked exchanges (Amir, 2015).

Hacking

One of the most "long-standing and well-publicised kinds of cybercrime is hacking (Furnell, 2010). The term "hacking" refers to any activity that involves acquiring or attempting to gain unauthorised access to information technology (IT) to steal data, manipulate data, or change a device's software or hardware (Clarke, Clawson & Cordell, 2003). Hacking began as a clandestine technical capability used to obtain access to a computer or networked systems to conduct risk and threat assessments. The term 'white hat' refers to hacking actions that are not criminal, whereas the word 'black hat' refers to any hacking activity that is criminal in nature (or attempt thereof). Hacking is used in the context of cryptocurrencies to acquire access to the private key, which is the password to a virtual wallet where the bitcoins are stored. To 'open' the wallet and take the cryptocurrency, the keys are used. Alternatively, the hacker might take over the bitcoin mining pool and use its whole computer capacity to mine money for themselves.

3. RESEARCH GAPS/FINDINGS

While there is quite a huge number of research on cryptocurrencies, and their usage for both legit and illegal purposes, very little research can be found on approaches to mitigating their use by cybercriminals. Nonetheless, some researchers have pointed out some approaches to mitigating the criminal use of bitcoins.

The Regulatory Environment

Tsukerman (2015) examines the situation of the Bitcoin regulatory environment from the perspective of the United States of America (USA). They divide the laws into two categories to help people comprehend the situation: those that safeguard Bitcoin users and those that address the broader societal implications of persons using Bitcoin for unlawful purposes like money laundering and terrorist financing (Tsukerman, 2015). Tu & Meredith (2015) add to Tsukerman's work by examining the barriers to successful Bitcoin regulation, which tackles the concerns of ownership, attribution, and vulnerability to theft that virtual currencies face. In February 2014, Wagstaff & Karpeles (2014) reported on the greatest Bitcoin theft at the Bitcoin exchange Mt Gox. This breach resulted in about a loss of US$ 450 million worth of bitcoins at the time.

Tu & Meredith (2015) identified reclaiming this stolen cash as a substantial risk to users. In contrast to traditional money transfer enterprises and financial organizations, cryptocurrency systems, according to Irwin & Turner (2018), are mostly unaffected by anti-money laundering and counter-terrorism financing (AML/CTF) legislation. Furthermore, these systems do not collect the essential Personal Identifiable Information (PII) to enable the adoption of tight financial transaction reporting processes aimed at preventing illicit financial activity and money laundering (Irwin & Turner, 2018).

Automated Software

Spagnuolo et al. (2014) established a framework for forensic investigation of such illegitimate Bitcoin transactions, as well as statistical modelling and autonomous software known as Bitiodine. This application parses the Blockchain technologies for transactions and accounts before aggregating, contextualizing, and displaying Bitcoin transaction graphs using data scraped from the web. The application of their approach to diverse case studies is an essential part of this literature.

These include looking at Silk Road Bitcoin activity and linked trades on the suspect Mt Gox exchange, as well as transactions by Silk Road's proprietor, Dread Pirate Roberts, aka Ross Ulbricht, and correlating web forum data with a blockchain ledger. The Cryptolocker ransomware investigation is maybe the most significant Bitiodine implementation. Bitiodine was utilized in the location of the CryptoLocker cluster(s) that belong to the malware developers (Spagnuolo et al, 2014). A classifier is then applied to these addresses, grouping the list of extorted addresses and automatically connecting Reddit usernames with Bitcoin addresses. Numisight and Maltego are two automated analysis tools identified by Furneaux (2018) that help visualize the Bitcoin graph and forensically analyse problematic addresses.

4. IMPLICATIONS FOR CYBER SAFETY IN AFRICA

Africa is the world's smallest cryptocurrency industry, but the market is constantly growing. The legal use of cryptocurrencies on the continent has the potential to stimulate transactions, particularly among people and small enterprises. Those are the users who behind the most recent rises in cryptocurrency transfers in South Africa, Nigeria, Ghana, and Kenya. However, Africa must be prepared for the hazards that digital currencies bring, including cyber frauds, organized crime, and financial crimes like money and crypto laundering. In 2020, South Africa recorded the world's largest cryptocurrency fraud. Hundreds of thousands of people were duped out of $588 million in Bitcoin through a Ponzi scheme perpetuated by Mirror Trading International. An even bigger cryptocurrency crime was uncovered in April 2021, by a South African company AfriCrypt, whose two founders stole $3.6 billion from investors in just a acouple of hours.

In terms on navigating the muddy waters of the cryptocurrency world, Africa has a very long way to go to catch up to the rest of the developed world. African governments seem oblivious of the true threat of cybercrime thus an absence in efforts to educate their citizens about the dangers that lurk on the internet. Africa must develop a sustainable risk plan, as well as appropriate legislation and cybersecurity rules, as well as a recovery strategy in the event that something goes wrong. They must conduct emergency drills, test their systems for flaws, and revise all government policies, including military policy. Complete mitigation against criminal cyberactivity is far from possible at the moment, even in the most developed countries, however, African governments must make the efforts, take the necessary steps forwards towards achieving this goal.

Change will be impossible until Africa adopts a new approach to cyber education about the hazards of accessing the internet without necessary security measures. Until then, African businesses will incur significant losses and will struggle to protect critical data from criminals. To make Africa's cyber environment secure enough for everyone to use, industry and governments must work together. Africa is home to some of the world's fastest-developing countries, yet due to its numerous economic and political issues, it is unable to keep up with current cybersecurity trends. It is a major target for hackers of all kinds due to a lack of competent people and cybersecurity knowledge.

5. IMPLICATIONS FOR PRACTICE, RESEARCH AND POLICIES

There is no silver bullet for cyber security challenges that blockchain and associated technologies can provide. They only reinforce current efforts to secure networks, communications, and data. To maintain irrevocable records, blockchain uses encryption and hashing, and many existing cyber security solutions use as well. To verify information or store encrypted data, the majority of present security methods rely on a single trusted authority. As a result, the system is open to attack, and numerous bad actors could concentrate their efforts on a single target to launch denial-of-service assaults, inject malicious data, or extort data via theft or blackmail. True blockchains have an advantage over existing security methods in that they are decentralised and do not require the authority or trust of a single organisation or network member. The system does not require trust since each node, or member, has a complete copy of all the historical information accessible, and additional data is only added to the chain of prior information by obtaining majority consensus.

The successful prosecution of such cybercrime requires global strategic and joint efforts by investigating authorities. More research is needed to:

a) identify the key challenges that cryptocurrencies pose to criminal justice systems in terms of investigation and prosecution;
b) determine the effectiveness of current criminal and procedural laws in effectively investigating and successfully prosecuting cryptocurrency-related crime;
c) improve international policing co-operation against cybercriminals;
d) improve co-operation between law enforcement and the private sector.

6. CONCLUSION

It's unknown how useful cryptocurrencies will be in the future as terrorist methods and cryptocurrencies evolve. Nonetheless, some recent advancements in cryptocurrency will make it easier for the most sophisticated terrorist groups to use them, and cryptocurrency use will be especially advantageous for actors who currently participate in international fundraising and criminal activities. According to research, if a single cryptocurrency emerges with widespread usage, better anonymity, increased security, and is subject to inconsistent regulation, the cryptocurrency's potential utility, as well as the possibility of terrorist organizations using it, will increase. Even if no such currency exists, terrorist groups will utilize it, but the amount of their usage will be determined by the currency's feasibility. Continued volatility and internal strife in the crypto world, the synergy between global law enforcement and the intelligence agencies, and changes in legislation and enforcement are all elements that tend to discourage use.

7. RECOMMENDATION FOR POLICY AND PRACTICES

For best policy development and practices, the following recommendations are proposed; the formation of superior international agencies to coordinate cryptocurrency interaction by defining norms, standards, quality control, and establishing permissions and prohibitions. These entities will also defend the rights of individuals and groups engaged in the crypto trade. The adoption of an intelligent system to monitor crypto activities, singling out suspicious activities based on deep machine learning while maintaining the autonomous nature of the currency is also highly recommended.

8. DIRECTION FOR FUTURE WORKS

Both risk-averse investors and the criminal underground are drawn to cryptocurrencies. Criminals are interested in them as an attack target, a source of payment, and a way to launder money. Cryptocurrencies empower criminals and provide them with numerous opportunities to invent new cybercrimes, according to regulators. Both sides are making improvements, according to one research. Criminals are exploiting new opportunities to elude control and develop new cybercrime services while law enforcement gradually implements new measures. Because of the recent substantial increase in the price of cryptocurrencies and the public's heightened interest in them, the years ahead will be very intriguing for further research in this sector.

REFERENCES

1. Amir, U. 2015. Phishing attack causes Bitcoin payment processor BitPay to lose $1.8m. HackRead, 19 September.
2. Bray, J. (2016). Anonymity, Cybercrime and the Connection to Cryptocurrency (Doctoral dissertation, Eastern Kentucky University).
3. Ciancaglini, V., Balduzzi, M., McArdle, R., & Rösler, M. (2015). The Deep Web. Trend Micro.
4. Clarke, Z, Clawson, J, Cordell, M, (2003), A brief History of Hacking, Historical Approaches to Digital Media, USA.
5. Fanusie, Y., & Robinson, T. (2018). Bitcoin laundering: an analysis of illicit flows into digital currency services. Center on Sanctions and Illicit Finance memorandum, January.
6. Furneaux, N. (2018). Investigating cryptocurrencies: understanding, extracting, and analyzing blockchain evidence. John Wiley & Sons.
7. Furnell, S. (2010) Jumping Security Hurdles. Computer Fraud & Security, 2010, 10-14.
8. Irwin, A. S., & Turner, A. B. (2018). Illicit Bitcoin transactions: challenges in getting to the who, what, when and where. Journal of money laundering control.
9. Naik, S. & Serumula, R. 2015. Dark Web thriving in SA. Saturday Star, 17 October 2015.
10. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, 21260.
11. Reddy, Eveshnie & Minnaar, Anthony. (2018). Cryptocurrency: a tool and target for cybercrime.
12. Schatt, D. (2014). Virtual Banking: A Guide to Innovation and Partnering. John Wiley & Sons.
13. Spagnuolo, M., Maggi, F., & Zanero, S. (2014). Bitiodine: Extracting intelligence from the bitcoin network. In International conference on financial cryptography and data security (pp. 457-468). Springer, Berlin, Heidelberg.
14. Tsukerman, M. (2015). The block is hot: A survey of the state of Bitcoin regulation and suggestions for the future. Berkeley Technology Law Journal, 30(4), 1127-1170.
15. Tu, K. V., & Meredith, M. W. (2015). Rethinking virtual currency regulation in the Bitcoin age. Wash. L. Rev., 90, 271.
16. Turner, A., & Irwin, A. S. M. (2018). Bitcoin transactions: a digital discovery of illicit activity on the blockchain. Journal of Financial Crime.
17. Van Mieghem, V., & Pouwelse, J. (2015). Anonymous online purchases with exhaustive operational security.
18. Wagstaff, J., & Karpeles, M. (2014). Mt. Gox bitcoin debacle: huge heist or sloppy glitch.